DOI 10.15276/imms.v14.no4.391
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 4, pp. 391-404

ЕКСПРЕС-АУДИТ ЯК ІНСТРУМЕНТ ОЦІНКИ ВРАЗЛИВОСТЕЙ В СИСТЕМАХ ОБРОБКИ ДАНИХ: ПІДХОДИ, МЕТОДИКИ ТА РЕКОМЕНДАЦІЇ

О. А. Сиропятов, Л. М. Тимошенко, І. В. Назарова, Н. Г. Козаченко

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044,Україна
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

Стаття присвячена дослідженню та розробці методики експрес-аудиту систем обробки даних на предмет захисту інформації. Основна увага приділена таким аспектам. По-перше, це порівняльний аналіз методів аудиту систем інформаційної безпеки. Проведено огляд і аналіз існуючих підходів до аудиту інформаційної безпеки з метою вибору найбільш придатних методів для використання в експрес-аудиті. Зроблено висновок, що для виконання експрес-аудиту найкраще комбінувати автоматизовані інструменти та аудит вразливостей для забезпечення ефективного виявлення загроз за мінімальний час та ресурси. По-друге, це розробка методики експрес-аудиту. Представлено підхід до швидкого отримання достовірної оцінки здатності системи обробки даних протистояти сучасним загрозам. Методика орієнтована на оперативне виявлення вразливостей та оцінку ризиків. Методика складається з послідовного ланцюжка блоків, кожен з яких містить етапи збору та обробки вхідної інформації, після чого отримані дані передаються до наступного блоку для подальшої обробки та використання. Методика дозволяє сформувати чітку структуру для оцінки поточного стану інформаційної безпеки, виявлення уразливих місць та своєчасного коригування політик безпеки з метою мінімізації потенційних ризиків. По-третє, це застосування запропонованої методики. Практично виконано експрес-аудит керуючого центру систем обробки даних підприємства, що активно проводить логістичні операції. На етапі аналізу розглянуто структуру системи, специфікацію обладнання, ліцензування та оновлення програмного забезпечення тощо. Надано практичні рекомендації щодо покращення процесів інформаційної безпеки на основі результатів експрес-аудиту. Результати дослідження показують можливість використовувати методику експрес-аудиту для швидкої оцінки стану безпеки інформаційних систем та для постійної оцінки безпеки, що дозволяє оперативно реагувати на нові загрози сьогодення.

Ключові слова: експрес-аудит, інформаційна безпека, системи обробки даних, методика аудиту, вразливості, автоматизовані інструменти, ризики

Вступ. У сучасних умовах стрімкого розвитку технологій та зростання кіберзагроз організації будь-якого масштабу опиняються перед необхідністю забезпечення надійного захисту даних. Зі збільшенням складності та витонченості кібератак традиційні підходи до інформаційної безпеки є недостатніми. У цьому контексті аудит СОД (систем обробки даних) на предмет захисту інформації є критично важливим інструментом, оскільки дозволяє не лише оцінити ефективність існуючих заходів захисту, але й виявити приховані вразливості, які можуть бути використані зловмисниками[1, 2].

В Україні через актуальні загрози сьогодення активно створюються відомчі та волонтерські системи обробки інформації, що базуються на різнотипному обладнанні, часто вживаному й отриманому через допомогу чи волонтерські ініціативи. Залучення пристроїв без повної історії експлуатації створює нові виклики для забезпечення безпеки [3-5]. За звичайних умов найкращим рішенням цієї проблеми був би традиційний аудит новостворених систем. Проте це тривалий і ресурсоємний процес, який не завжди доцільний у сучасних реаліях.

У зв’язку з цим виникає потреба у розробці доступних методик експрес-аудиту, які дозволять швидко та економічно оцінити безпеку систем обробки даних. Це

забезпечить надійний захист критичної інформації та оперативне реагування на потенційні ризики в умовах обмежених ресурсів. Отже, сьогодні важливо знайти баланс між швидкістю, точністю та економічністю аудиторських перевірок, щоб ефективно мінімізувати ризики та забезпечити належний захист даних[6, 7].

Метою дослідження є обґрунтування та розробка методики експрес-аудиту для оцінки безпеки інформаційних систем, сформованих на базі різнотипного обладнання, з урахуванням сучасних загроз та обмежених ресурсів.

Для досягнення мети необхідно вирішити наступні *завдання*.

1. Провести порівняльний аналіз основних методів аудиту СОД на предмет захисту інформації для вибору найвідповідніших в рішенні поставленої задачи.

2. Розробити методику швидкого отримання достовірної оцінки здатності системи обробки даних протистояти сучасним загрозам.

3. Виконати експрес-аудит реальної системи обробки даних за розробленою методикою.

4. Розробити рекомендації щодо використання результатів дослідження для покращення безпеки систем обробки даних.

Порівняльний аналіз основних методів аудиту СОД на предмет захисту інформації для використання в методиці експрес-аудиту. Аудит СОД на предмет захисту інформації – це процес перевірки поточного стану інформаційного захисту без впровадження змін. Це діагностичний етап, метою якого є виявлення слабких місць, оцінка ризиків та визначення відповідності стандартам. У сучасних умовах аудит СОД на предмет захисту інформації може здійснюватися різними методами, кожен з яких має свої особливості [1,4,6]. Проведемо порівняльний аналіз основних методів аудиту СОД на предмет захисту інформації для вибору найвідповідніших з подальшим використанням в методиці експрес-аудиту.

1. Ручний аудит (Manual Audit). Цей метод містить паперовий аналіз системи фахівцями вручну. Він охоплює перевірку конфігурацій, прав доступу, а також інших аспектів безпеки. Ручний аудит дозволяє детально проаналізувати складні системи та виявити вразливості, які можуть бути пропущені автоматичними інструментами. Такий підхід корисний для виявлення нестандартних або унікальних вразливостей та надає глибше розуміння специфіки системи.

2. Автоматизовані інструменти аудиту (Automated Audit Tools). Використання спеціалізованих програмних рішень для автоматизованого сканування системи на наявність відомих вразливостей. Програми, зокрема, Nessus, OpenVAS або Qualys, здатні швидко виявити слабкі місця в конфігураціях мережевих пристроїв, серверів і додатків. Цей метод підходить для регулярних перевірок у великих і складних системах.

3. Аудит конфігурацій і політик (Configuration and Policy Audit). Це оцінка конфігурацій і політик безпеки, зокрема, налаштування серверів, мережевих пристроїв і додатків. Метою є виявлення неправильних або ненадійних налаштувань, які можуть створити вразливості. Цей аудит також включає перевірку відповідності політик безпеки (наприклад, політики доступу, шифрування та використання паролів) внутрішнім і зовнішнім вимогам безпеки.

4. Аналіз журналів і подій (Log and Event Analysis). Аналіз системних журналів і записів подій для виявлення підозрілих дій, несанкціонованих спроб доступу або аномалій, які можуть свідчити про наявність вразливостей у системі. Цей метод допомагає не лише виявляти вразливості на етапі експлуатації, а також виявляти можливі атаки на ранніх стадіях.

5. Аудит вразливостей (Vulnerability Audit). Спеціалізований аудит, метою якого є виявлення відомих вразливостей у системі. Цей метод містить використання як автоматичних інструментів, так і ручних перевірок для сканування системи на

наявність слабких місць, які можуть використовуватись для атак. При цьому оцінюють також актуальність оновлень і патчів безпеки.

Критерії оцінки методів аудиту. Вибір оптимальних методів аудиту визначають за трьома критеріями, оціненими за 5-бальною шкалою:

- достовірність (чи виявляє метод усі вразливості);
- швидкість(час на проведення аудиту);
- ресурсоємність(необхідні ресурси для виконання аудиту).

Оцінки методів аудиту наведено в таблиці 1.

Таблиця 1.

Оцінки методів аудиту на основі обраних критеріїв

Метод аудиту	Достовірність (1-5)	Швидкість (1-5)	Ресурсоємність (1-5)	Загальна оцінка (1-5)
Ручний аудит (Manual Audit)	5	1	3	3
Автоматизовані інструменти аудиту	4	4	4	4
Аудит конфігурацій і політик безпеки	4	2	3	3
Аналіз журналів і подій (Log Review Audit)	3	3	3	3
Аудит вразливостей (Vulnerability Assessment Audit)	5	3	4	4

З таблиці 1 слідує, що автоматизовані інструменти аудиту та аудит вразливостей мають найвищу оцінку, що робить їх найбільш ефективними для виявлення загроз. Ручний аудит забезпечує високу достовірність, але є ресурсоємним і повільним. Отже, для виконання експрес-аудиту найкраще комбінувати автоматизовані інструменти та аудит вразливостей для забезпечення ефективного виявлення загроз за мінімальний час та ресурси.

Розробка методики швидкого отримання достовірної оцінки здатності системи обробки даних протистояти сучасним загрозам. Розробка методу експрес-аудиту для керуючого центру СОД підприємства, що активно проводить логістичні операції, має на меті швидке виявлення потенційних загроз та вразливостей. Ефективне і безвідмовне функціонування керуючого центру СОД критично важливе, оскільки будь-які збої, порушення в роботі інформаційних потоків або втрата даних можуть мати важкі наслідки для людського життя та фінансових ресурсів. Проведення експрес-аудиту дає змогу оперативно оцінити стан безпеки системи та вчасно вжити необхідних заходів для забезпечення безпеки даних і ресурсів підприємства.

1. Оцінка основних загроз та вразливостей інформаційної безпеки керуючого центру СОД.

Методика експрес-аудиту передбачає виявлення і оцінку основних загроз і вразливостей керуючого центру СОД[3,7,8]. Особливу увагу приділено таким загрозам, як несанкціонований доступ до даних, порушення конфіденційності, цілісності та доступності інформації. Важливою складовою є перевірка ефективності існуючих засобів захисту та виявлення слабких місць в інфраструктурі СОД, які можуть стати ціллю для атак зловмисників.

2. Основні етапи методики експрес-аудиту.

Методика експрес-аудиту складається з кількох етапів, кожен з яких сприяє ефективному виявленню загроз і вразливостей:

– ідентифікація об'єкту захисту інформації, аналіз основних активів СОД, які вимагають захисту;

– оцінка загроз і вразливостей, перевірка загроз і вразливостей СОД;

– аналіз ефективності існуючих засобів захисту, оцінка рівня захисту інформаційних потоків та політик безпеки в інфраструктурі;

– рекомендації щодо поліпшення рівня захисту СОД.

3. Методи та інструменти для проведення експрес-аудиту.

Для швидкого виявлення вразливостей у мережевій інфраструктурі, базах даних і компонентах СОД використовують спеціалізовані інструменти, зокрема:

– сканери вразливостей OpenVAS для виявлення слабких місць у системах;

– аналіз вразливостей виконують на платформі ELK Stack (Elasticsearch, Logstash, Kibana);

– інструменти тестування на проникнення Nmap для виявлення можливості несанкціонованого доступу;

– програмне забезпечення для моніторингу безпеки FlexNet, яке дозволяє вчасно відслідковувати інциденти.

4. Оцінка ефективності методики експрес-аудиту.

Ефективність методики оцінюється за кількістю виявлених загроз і вразливостей, а також за швидкістю їх виявлення та точністю. Важлива характеристика - це здатність методики оперативно реагувати на критичні ситуації і забезпечити своєчасне прийняття рішень для мінімізації ризиків. Оцінка містить також здатність методики забезпечити максимальну точність і швидкість при мінімальних витратах часу [7].

Методика експрес-аудиту керуючего центру СОД. Методика складається з послідовного ланцюжка блоків, кожен з яких містить етапи збору та обробки вхідної інформації, після чого отримані дані передаються до наступного блоку для подальшої обробки та використання.

1. Блок вхідної інформації. Цей блок збирає всі вихідні дані про керуючий центр СОД важливі для подальшого аналізу:

– структурна схема керуючого центру СОД - візуальне відображення маршрутів інформаційних потоків, зв'язок компонентів системи;

– специфікація обладнання - список всіх серверів, маршрутизаторів, мережевих сховищ та інших ключових компонентів, включаючи дані про виробника, версії, конфігурацію;

– інформація про ліцензії - дані про всі використовувані ліцензії для програмного забезпечення(ПЗ), операційних систем, мережевих пристроїв та оновлення ліцензій;

– сервісна служба оновлень - інформація про механізми оновлення ПЗ, автоматизацію процесів та терміни оновлень.

Алгоритм:

Крок 1. Використання автоматизованих систем інвентаризації обладнання Nmap.

Крок 2. Сканування ліцензій та оновлень за допомогою спеціалізованих рішень FlexNet.

2. Блок розподілу "ваги" елементів**,** де кожному елементу системи присвоюється "вага" у контексті забезпечення інформаційної безпеки.

Наприклад. Критичні сервери - висока вага, маршрутизатори - середня, периферійні пристрої - низька вага.

Алгоритм:

Крок 1. Використання критеріїв, заснованих на важливості елементів для бізнес-процесів, чутливості даних і рівні доступу.

Крок 2. Застосування шкали оцінок (від 1 до 5) для визначення ваги кожного компонента.

3. Блок аудиту елементів.

Цей блок проводить безпосередній аудит елементів системи, використовуючи комбінацію автоматизованих інструментів та методів аналізу вразливостей.

Автоматизовані інструменти: використання сканерів безпеки OpenVAS для виявлення вразливостей в обладнанні та ПЗ.

Аналіз вразливостей: використання платформи ELK Stack (Elasticsearch, Logstash, Kibana).

Алгоритм:

Крок 1. Сканування всіх елементів на вразливості з використанням автоматизованих інструментів.

Крок 2. Виявлення критичних вразливостей на основі ваги елементів.
Крок 3. Аналіз журналів і подій для виявлення слідів атак.

4. Блок збору результатів аудиту.

На цьому етапі збирають всі результати аудиту по кожному елементу та агрегують для отримання комплексної картини стану безпеки керуючого центру СОД:
– автоматичний збір звітів із систем сканування вразливостей;
– оцінка ризику для кожного елемента на основі виявлених вразливостей та їх "ваги";
– пріоритизація: вагоміші елементи з критичними вразливостями отримують максимальний пріоритет для усунення загроз.
Алгоритм:
Крок 1. Систематизація даних у звіті з указанням вразливостей, рівня їх критичності та потенційних збитків.
Крок 2. Створення списку пріоритетних завдань щодо виправлення.

5. Результатний блок - це фінальний блок, який готує комплексний висновок за результатами аудиту, виводить загальну оцінку рівня інформаційної безпеки керуючого центру СОД та дає рекомендації щодо поліпшення.

5.1. Оцінка загального рівня ризику: використання методу зваженої оцінки всіх виявлених вразливостей. Для того, щоб шкала оцінки сумарних ризиків мала сенс і була обґрунтована, можна використовувати наступні підходи [9, 10].

Обґрунтування через концентрацію ризиків. Ризики з високими значеннями можуть мати великий вплив на безпеку, а їх сумарне значення відображає загальний стан інформаційної безпеки. Використовуючи підхід з бальною шкалою, можна згрупувати ризики за рівнями та призначити чіткі порогові значення, які будуть вказувати на різницю в ступені загрози для системи.

Обґрунтування через практичну значущість. Встановлення порогових значень на основі практичної значущості ризиків у контексті їхнього впливу на діяльність організації, що дозволяє оцінити необхідність негайного вживання заходів для мінімізації збитків.

Розглянемо приклад шкали для сумарних ризиків. Низький рівень (0-10 балів) - ризики, які не мають значного впливу на систему, їх можна усунути в рамках звичайного контролю безпеки. Середній рівень (11-20 балів) - ризики, які можуть вплинути на систему в певних умовах, їх потрібно виправити, але вони не вимагають термінових заходів. Високий рівень (21-30 балів) - ризики, які вимагають швидкої реакції, через можливі серйозні збитки або порушення роботи системи, усунення цих ризиків має стати пріоритетом. Критичний рівень (31 і більше балів) - дуже високі ризики, які є безпосередньою загрозою для безпеки СОД. Ці ризики потрібно усунути негайно, оскільки їх реалізація може призвести до значних збитків або витоку даних. Ця шкала допомагає зрозуміти, які ризики вимагають негайної уваги, а які можна відкласти. Система оцінок і порогових значень допомагає зробити пріоритети в усуненні уразливостей прозорішими і структурованими.

5.2. Висновки про ефективність заходів захисту: оцінка поточної стратегії захисту інформації керуючого центру СОД та запропоновані заходи з її оптимізації.

5.3. Рекомендації щодо покращення: пропозиції по впровадженню додаткових заходів захисту (наприклад, покращення оновлень, використання захищених протоколів тощо).
Алгоритм**:**
Крок 1. Фінальна інтеграція всіх даних у комплексний звіт.
Крок 2. Порівняння з попередніми результатами аудиту (якщо доступні) для визначення динаміки поліпшень.

Узагальнений алгоритм реалізації експрес-аудиту наведено на рисунку 1.

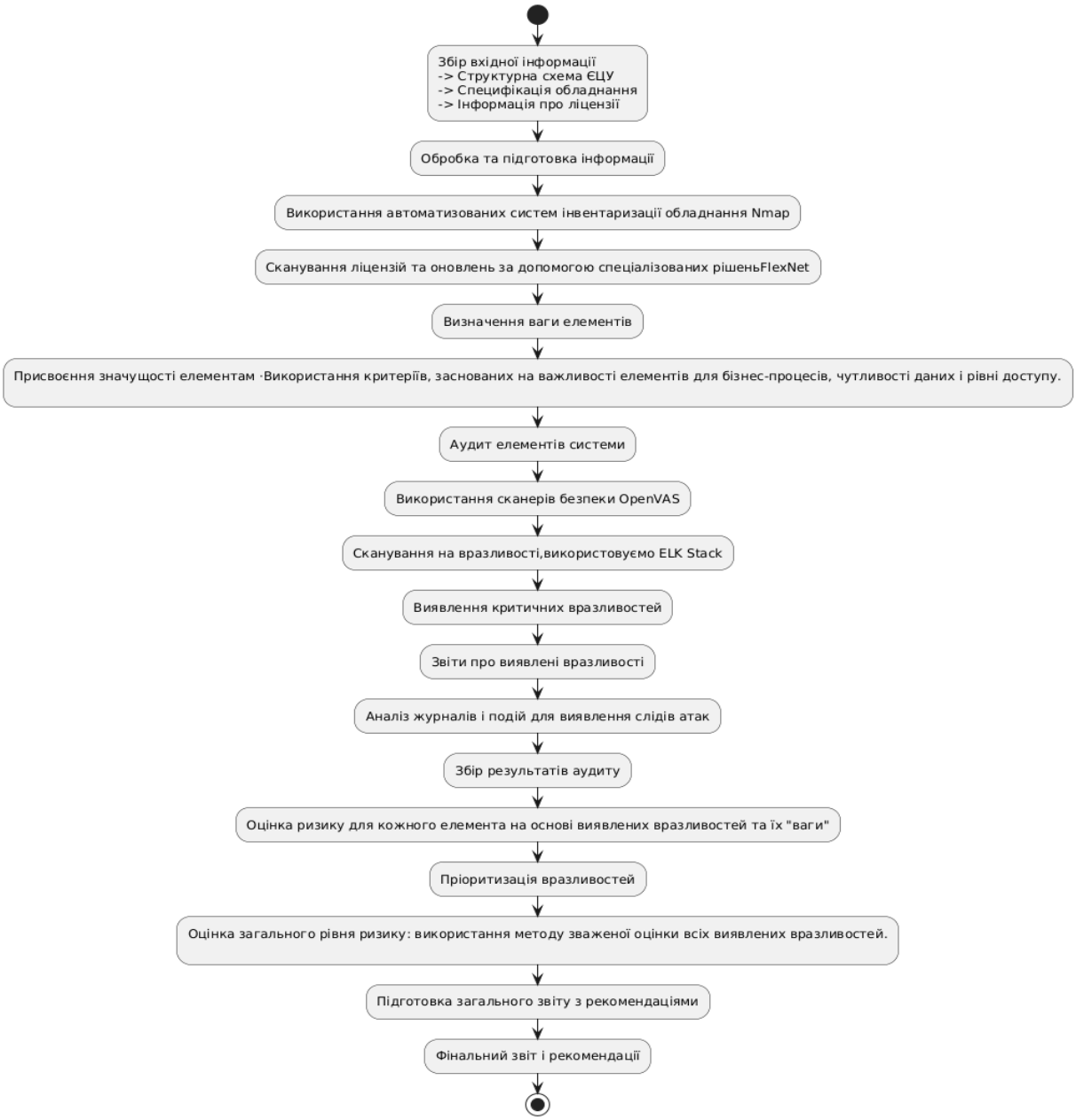

Рис. 1 Алгоритм реалізації експрес-аудиту

Отже, таким чином буде досягнута основна мета розробленої методики — визначення кроків для швидкої та достовірної оцінки здатності керуючого центру СОД протистояти сучасним загрозам. Методика дозволяє сформувати чітку структуру для оцінки поточного стану інформаційної безпеки, виявлення уразливих місць та своєчасного коригування політик безпеки з метою мінімізації потенційних ризиків.

Експрес-аудит керуючого центру СОД за розробленою методикою.

1. Блок вхідної інформації.

Збір вихідних даних про керуючого центру СОД

На цьому етапі зібрано основні дані про керуючий центр СОД, включаючи структуру, специфікації обладнання, інформацію про ліцензії та оновлення програмного забезпечення.

1.1. Структурна схема керуючого центру СОД. З метою забезпечення конфіденційності внесено деякі зміни в структурну схему та специфікації обладнання, які не впливають на хід дослідження (рисунок 2).

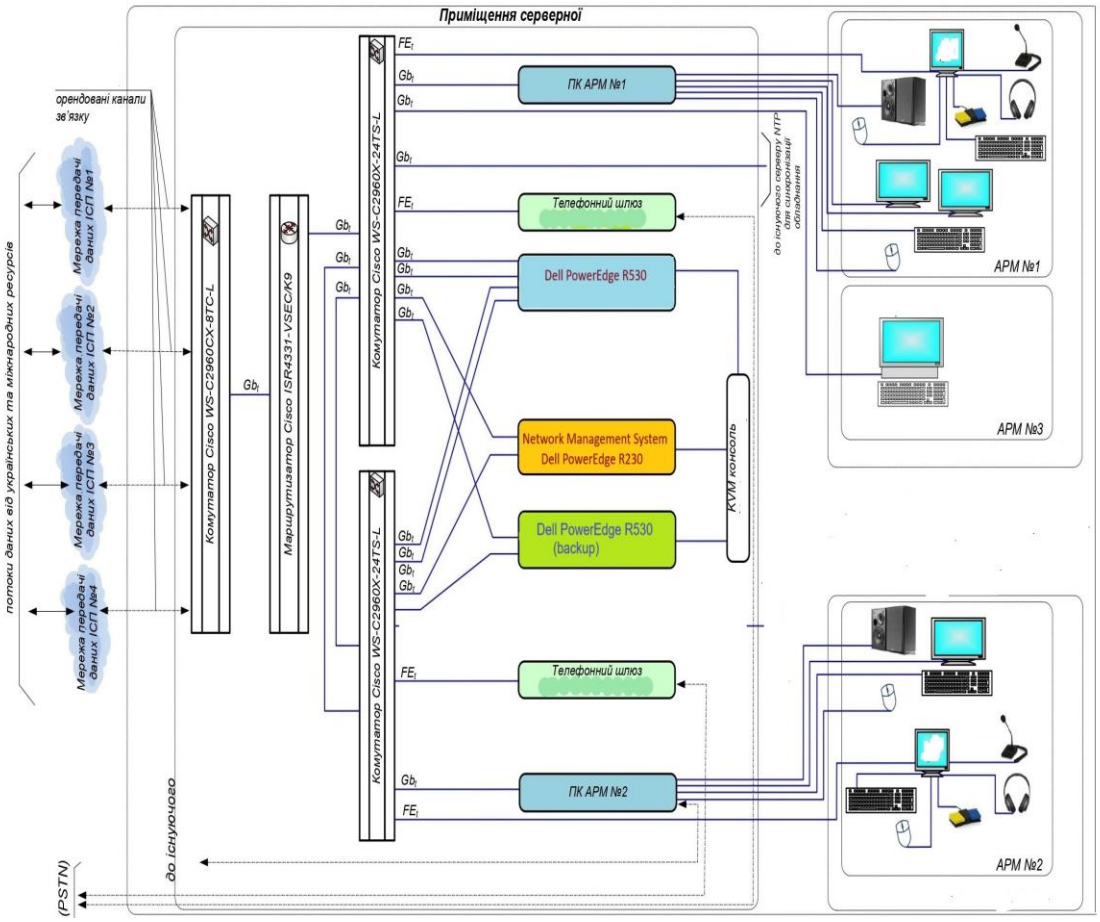

Рис.2 Структурна схема керуючого центру СОД

1.2. Специфікація обладнання:
- Сервери DELL PowerEdge R530, PowerEdge R230
- Маршрутизатор ISR4331-VSEC/K9
- Комутатори WS-C2960X-24TS-L, Cisco WS-C2960CX-8TC-L
- Сервери Supermicro SYS-5018R-M

1.3. Інформація по ліцензіях ПЗ:
- IPMI 2.0
- Dell OpenManage Essentials
- Dell OpenManage Mobile
- Dell OpenManage Power Center

1.4. Інформація по оновленням ПЗ:
- Dell SupportAssist і DELL Update Utility
- Cisco WS-C2960CX-8TC-L, WS-C2960X-24TS-L і ISR4331-VSEC/K9
- Шифрування: DES, 3DES, AES-128/256
- Аутентифікація: RSA, ECDSA
- Цілісність: MD5, SHA
- Cisco Smart Licensing та Cisco DNA Center

1.5. Заходи безпеки:
- Резервування: кластеризація серверів, резервування шлюзів.
- Шифрування даних: протоколи TLS та IPSec.
- Фізична захист: захищені приміщення з обмеженим доступом.
- Кілька провайдерів: підключення до кількох провайдерів для надійності зв'язку.

1.6. Результати застосування автоматизованих систем інвентаризації обладнання Nmap наведено в таблиці 2.

Таблиця 2.

Результати сканування з використанням автоматизованих систем інвентаризації

Найменування обладнання	Тип обладнання	Внутрішній IP-адрес*	Зовнішній IP-адрес*	Порт	Протокол	Сервіс
Комутатор Cisco WS-C2960CX-8TC-L	Комутатор	192.168.1.1	203.0.113.10	80	TCP	HTTP
Маршрутизатор Cisco ISR4331-VSEC/K9	Маршрутизатор	192.168.1.2	203.0.113.11	179	TCP	BGP
Комутатор Cisco WS-C2960X-24TS-L	Комутатор	192.168.1.3	-	80	TCP	HTTP
Комутатор Cisco WS-C2960X-24TS-L	Комутатор	192.168.1.4	-	80	TCP	HTTP
Сервер DELL PowerEdge R530	Сервер	192.168.1.5	-	443	TCP	HTTPS
Сервер DELL PowerEdge R230	Сервер	192.168.1.6	-	8080	TCP	HTTP
Телефонний шлюз PGW-1125	Шлюз	192.168.1.7	-	5060	UDP	SIP
GSM VoIP-шлюз	Шлюз	192.168.1.8	-	5060	UDP	SIP
KVM консоль ATEN CL-1000M	Консоль	192.168.1.9	-	22	TCP	SSH

*З метою забезпечення конфіденційної інформації реальні дані у стовпцях "Внутрішня IP-адреса" та "Зовнішня IP-адреса" змінені.

1.7. Результати сканування ліцензій та оновлень за допомогою FlexNet наведено в таблиці 3.

Таблиця 3.

Результати сканування ліцензій та оновлень за допомогою спеціалізованих рішень

Обладнання	ПЗ/Ліцензія	Версія	Оновлення
DELL PowerEdge R530	IPMI 2.0	Вбудована	Оновлення через iDRAC
	Dell OpenManage Essentials	Безкоштовна	Оновлення через DELL SupportAssist
	Dell OpenManage Mobile	Включена	Оновлення через DELL SupportAssist
	Dell OpenManage Power Center	Включена	Оновлення доступні на сайті DELL
DELL PowerEdge R230	IPMI 2.0	Вбудована	Оновлення через iDRAC
	Dell OpenManage Essentials	Безкоштовна	Оновлення через DELL SupportAssist
	Dell OpenManage Mobile	Включена	Оновлення через DELL SupportAssist
	Dell OpenManage Power Center	Включена	Оновлення доступні на сайті DELL
Cisco WS-C2960CX-8TC-L	Cisco IOS	15.2(4)E	Оновлення через Cisco Smart Licensing
Cisco WS-C2960X-24TS-L	Cisco IOS	15.2(4)E	Оновлення через Cisco Smart Licensing
Cisco ISR4331-VSEC/K9	Cisco IOS	16.9(4)	Оновлення через Cisco Smart Licensing

Завдяки скануванню виявлено, що деякі пристрої вимагають оновлення програмного забезпечення для підвищення рівня безпеки.

2. Блок розподілу ваги елементів

Дані щодо розподілу "ваги" елементів наведено в таблиці 4.

Таблиця 4.

Таблиця розподілу "ваги" елементів системи для забезпечення інформаційної безпеки

Елемент системи	Критичність (1-5)	Вразливість (1-5)	Наслідки порушення (1-5)	Середнє (вага)
Сервери DELL PowerEdge R530	5	4	5	4.67
Сервери DELL PowerEdge R230	4	3	4	3.67
Cisco WS-C2960CX-8TC-L	3	4	3	3.33
Cisco WS-C2960X-24TS-L	4	3	3	3.33
Cisco ISR4331-VSEC/K9	4	4	4	4.00

3. Блок аудиту елементів

Аналіз безпеки елементів керуючого центру СОД виконано за допомогою сканерів безпеки OpenVAS та аналізу журналів подій на платформі ELK.

Результат використання сканерів безпеки OpenVAS для виявлення вразливостей в обладнанні та програмному забезпеченні наведено в таблиці 5.

Таблиця 5.

Результат використання сканерів безпеки OpenVAS для виявлення вразливостей

Елемент системи	Уразливість	Оцінка уразливості (1-5)	Статус виправлення	Шифр уразливості
Cisco ISR4331-VSEC/K9	Уразливість у протоколі шифрування	3	Виправлено	CVE-2023-1234
Cisco WS-C2960CX-8TC-L	Слабкий алгоритм аутентифікації	2	Очікує виправлення	CVE-2023-2345
Cisco WS-C2960X-24TS-L	Уразливість до міжмережевих атак	4	В процесі виправлення	CVE-2023-3456
Dell PowerEdge R530	Уразливість в iDRAC	3	Виправлено	CVE-2023-4567
Dell PowerEdge R230	Недостатня захист конфіденційності	4	В процесі виправлення	CVE-2023-5678

Аналіз журналів подій на платформі ELK показує деталі активності в мережі та виявлені потенційно небезпечні події наведено в таблиці 6.

Таблиця 6.

Аналіз журналів подій на платформі ELK

Параметр	Опис	Дані за 72 години	Аномалії/Проблеми	Обладнання з аномаліями
Мережеві логи	Аналіз обсягів переданих даних та типів трафіку.	Вхідний трафік: 1,120 ГБ / Вихідний трафік:950 ГБ	Незначні сплески трафіку в нічний час.	Cisco ISR4331-VSEC/K9
Логи безпеки	Записи про спроби авторизації та доступи.	180 спроб авторизації З них 12 невдалих	Підвищена активність доступу з-за кордону.	Сервери Dell PowerEdge R530, R230
Системні логи	Повідомлення про помилки серверів та пристроїв.	28 критичних помилок на Dell R530 12 попереджень на Cisco ISR	Декілька помилок у періоди підвищеного навантаження на сервер.	Dell PowerEdge R530, Cisco ISR4331-VSEC/K9
Логи застосунків	Час відгуку застосунків, помилки баз даних.	Середній час відгуку: 450 мс Максимум: 1,000 мс	Відхилення за часом відгуку під час пікових навантажень.	Dell PowerEdge R230
Моніторинг пропускної здатності	Рівень використання каналів передачі даних.	Середнє використання: 70% Пікове використання: 92%	Часті перевантаження на каналах під час зміни потоків даних	Cisco ISR4331-VSEC/K9
Аналіз трафіку за часом доби	Піки та мінімуми у навантаженні в різний час доби.	Пік навантаження: 8-10 годин та 17-19 годин Мінімум: 02-05 годин	Навантаження перевищує оптимум у робочі години.	Cisco ISR4331-VSEC/K9

Виявлені уразливості на основі аналізу платформи ELK відображені в таблиці 7.

Таблиця 7.

Виявлені уразливості на базі аналізу платформи ELK

Ідентифікатор вразливості	Опис уразливості	Зачеплене обладнання	Критичність	Джерело даних
VULN-01	Незначні сплески трафіку в нічний час	Cisco ISR4331-VSEC/K9	Низька	Мережеві логи
VULN-02	Підвищена активність доступу з-за кордону	Dell PowerEdge R530, R230	Середня	Логи безпеки
VULN-03	Критичні помилки сервера в періоди підвищеного навантаження	Dell PowerEdge R530	Висока	Системні логи
VULN-04	Відхилення за часом відгуку при пікових навантаженнях	Dell PowerEdge R230	Середня	Логи застосунків
VULN-05	Часті перевантаження на каналах передачі даних	Cisco ISR4331-VSEC/K9	Середня	Моніторинг пропускної здатності
VULN-06	Перевищення оптимального рівня навантаження в робочі години	Cisco ISR4331-VSEC/K9	Низька	Аналіз трафіку за часом доби

Кожній уразливості присвоєно унікальний ідентифікатор (наприклад, VULN-01, VULN-02), що можна використовувати для посилань в інших розділах звіту або в рекомендаціях, що також спростить навігацію за результатами аудиту.

4. Блок збору результатів аудиту

Після виконання аудиту проведено аналіз вразливостей та рекомендацій щодо їх виправлення. Звіт з результатами наведено в таблиці 8.

Таблиця 8.

Аналіз вразливостей та рекомендації по їх виправленню

Елемент системи	**Уразливість**	**Оцінка**	**Шифр**	**Рекомендації**	**Статус виправлення**	**Примітки**	**Критичність**
Cisco ISR4331-VSEC/K9	Уразливість у протоколі шифрування	3	CVE-2023-1234	Оновити ПЗ та протоколи шифрування	Виправлено	Виправлення реалізоване у версії 15.3.2	Низька
Cisco WS-C2960CX-8TC-L	Слабкий алгоритм аутентифікації	2	CVE-2023-2345	Впровадити більш сильний алгоритм аутентифікації	Очікує виправлення	Планується виправлення в наступному оновленні	Середня
Cisco WS-C2960X-24TS-L	Уразливість до міжмережевих атак	4	CVE-2023-3456	Застосувати правила міжмережевого екрану	В процесі виправлення	Затверджено рішення, реалізація в плані	Висока
Dell PowerEdge R530	Уразливість в iDRAC	3	CVE-2023-4567	Провести аудит безпеки та оновлення	Виправлено	Успішно реалізовано, підтверджено тестами	Низька
Dell PowerEdge R230	Недостатня захист конфіденційності	4	CVE-2023-5678	Покращити конфіденційність даних	В процесі виправлення	Необхідно впровадження нових протоколів	Висока
Cisco ISR4331-VSEC/K9	Часті перевантаження на каналах передачі даних	3	VULN-05	Оптимізувати використання каналів передачі даних	Виправлено	Спостерігається покращення після змін	Середня
Dell PowerEdge R230	Відхилення за часом відгуку при пікових навантаженнях	4	VULN-04	Поліпшити продуктивність серверів	В процесі виправлення	Аналіз продуктивності триває	Середня
Dell PowerEdge R230	Уразливість у програмному забезпеченні	4	VULN-02	Оновити ПЗ до останньої версії	В процесі виправлення	Проводиться аудит версій	Висока
Cisco WS-C2960CX-8TC-L	Вразливість у механізмі авторизації	3	VULN-06	Впровадити додаткові заходи аутентифікації	Очікує виправлення	Визначено можливості для впровадження	Середня

Перелік пріоритетних завдань щодо виправлення зазначених вразливостей наведено в таблиці 9.

Таблиця 9.

Перелік пріоритетних завдань щодо виправлення

№	Елемент системи	Завдання	Причина	Термін виконання
1	Cisco WS-C2960X-24TS-L	Впровадити політики безпеки для управління доступом до обладнання. Налаштувати доступ лише для авторизованих користувачів, перевірити наявність усіх прав доступу.	Високий ризик від несанкціонованого доступу (оцінка уразливості: 4)	Протягом 3-х днів
2	Dell PowerEdge R230	Виконати шифрування даних на жорстких дисках сервера та впровадити двофакторну аутентифікацію для доступу до конфіденційних даних.	Недостатня захист конфіденційності (оцінка уразливості: 4)	Протягом 3-х днів
3	Cisco ISR4331-VSEC/K9	Оновити прошивку маршрутизатора до останньої версії, включаючи всі патчі безпеки. Реалізувати IPS для виявлення та блокування атак.	Уразливість в попередній версії (оцінка уразливості: 3)	Протягом 1 тижня
4	Cisco WS-C2960CX-8TC-L	Впровадити систему моніторингу трафіку та журналювання подій, налаштувати оповіщення про підозрілу активність.	Високий ризик від зловмисних атак (оцінка уразливості: 3)	Протягом 1 тижня
5	Dell PowerEdge R530	Провести повний аудит безпеки програмного забезпечення, впровадити регулярні оновлення та перевірки конфігурації системи iDRAC.	Уразливість в системі управління (оцінка уразливості: 3)	Протягом 1 тижня
6	Cisco ISR4331-VSEC/K9 (повторно)	Оптимізувати правила маршрутизації та налаштувати QoS для забезпечення стабільності та безпеки трафіку.	Часті перевантаження на каналах передачі даних (оцінка уразливості: 3)	Протягом 1 тижня
7	FlexNet	Провести навчання персоналу з використання ПО FlexNet для покращення управління ліцензіями та безпеки.	Недостатнє знання користувачів про функціонал ПО (оцінка уразливості: 2)	Протягом 1 місяця
8	Cisco WS-C2960CX-8TC-L	Впровадити більш сильний алгоритм аутентифікації для покращення безпеки.	Слабкий алгоритм аутентифікації (оцінка уразливості: 2)	Протягом 1 тижня
9	Dell PowerEdge R230	Поліпшити продуктивність серверів, зменшити відхилення за часом відгуку при пікових навантаженнях.	Відхилення за часом відгуку при пікових навантаженнях (оцінка уразливості: 4)	Протягом 1 тижня
10	Cisco ISR4331-VSEC/K9	Оптимізувати використання каналів передачі даних, зменшити часті перевантаження.	Часті перевантаження на каналах передачі даних (оцінка уразливості: 3)	Протягом 1 тижня

5.Результатний блок

5.1. Оцінка загального рівня ризику.

Ризики по обладнанню наведено у таблиці 10. Оцінка дорівнює 29 балів (високий рівень) — необхідно негайно усунути виявлені уразливості для уникнення важких порушень функціонування системи.

Таблиця 10.

Ризики по обладнанню

Елемент системи	Оцінка уразливості	Критичність	Ризик	Рекомендації	Статус виправлення
Cisco ISR4331-VSEC/K9	3	Середня	6	Оптимізувати правила маршрутизації та налаштувати QoS	В процесі виправлення
Cisco WS-C2960CX-8TC-L	2	Середня	4	Впровадити більш сильний алгоритм аутентифікації	Очікує виправлення
Cisco WS-C2960X-24TS-L	4	Висока	8	Впровадити політики безпеки для управління доступом	В процесі виправлення
Dell PowerEdge R530	3	Низька	3	Провести повний аудит безпеки програмного забезпечення	Виправлено
Dell PowerEdge R230	4	Висока	8	Виконати шифрування даних та впровадити двофакторну аутентифікацію	В процесі виправлення

Ризики по вразливостям наведено у таблиці 11. Оцінка дорівнює 26 балам (високий рівень) — ці вразливості можуть призвести до серйозних наслідків, тому їх усунення є пріоритетом. Ці ризики вимагають негайної уваги та дій для зменшення потенційних збитків.

Таблиця 11.

Ризики по уразливостям

Уразливість	Оцінка уразливості	Критичність	Ризик	Рекомендації	Статус виправлення
VULN-01	1	Низька	1	Моніторити сплески трафіка	Немає необхідності
VULN-02	2	Середня	4	Зменшити доступ з-за кордону	В процесі виправлення
VULN-03	4	Висока	8	Провести аудит серверних помилок	Виправлено
VULN-04	3	Середня	6	Оптимізувати продуктивність серверів	В процесі виправлення
VULN-05	3	Середня	6	Оптимізувати використання каналів передачі даних	Виправлено
VULN-06	1	Низькя	1	Аналіз трафіку за часом доби	Немає необхідності

5.2. Оцінка поточної стратегії керуючого центру СОД.

Сильні сторони - наявність базових заходів захисту, контроль доступу, резервне копіювання даних та системи моніторингу, регулярні оновлення систем, обізнаність персоналу з питань інформаційної безпеки.

Слабкі сторони - відсутність комплексної стратегії управління інформаційною безпекою, недостатня реакція на інциденти, низький рівень захисту критичних систем.

5.3. Рекомендації щодо покращення інформаційної безпеки керуючого центру СОД: впровадити автоматизовані системи для моніторингу та установки оновлень; удосконалити існуючу систему моніторингу для виявлення загроз в реальному часі; впровадити багатофакторну аутентифікацію для всіх користувачів, особливо для критичних систем; проводити регулярні внутрішні та зовнішні аудити безпеки; розробити та підтримувати актуальний план реагування на інциденти, що включає чіткі інструкції по діям при загрозах.

Рекомендації щодо використання результатів дослідження щодо покращення безпеки систем обробки даних.

1. Впровадження експрес-аудиту. Результати дослідження показують, що можливо використовувати методику експрес-аудиту для швидкої оцінки стану безпеки систем обробки даних. Це дозволить оперативно виявляти потенційні ризики та своєчасно реагувати на зміни без великих витрат.

2. Оптимізація процесу аудиту. Для підвищення ефективності можна автоматизувати деякі етапи аудиту, що зменшить час перевірки та підвищить точність результатів.

3. Регулярний моніторинг. Можливо використовувати методику експрес-аудиту для постійної оцінки безпеки, що дозволяє оперативно реагувати на нові загрози.

4. Аналіз економічної доцільності. Важливо оцінювати ефективність аудиту з точки зору витрат, щоб забезпечити баланс між високим рівнем безпеки та наявними ресурсами.

Ці рекомендації допоможуть покращити процеси безпеки та зменшити ризики без значних витрат.

Висновки. Розроблено експрес-метод виявлення та оцінки основних загроз і вразливостей у системах обробки даних. Проведено огляд та аналіз існуючих підходів до аудиту інформаційної безпеки з метою вибору найвідповіднійших для поставленого завдання. За результатами аналізу зроблено висновок, що для проведення експрес-аудиту найкраще поєднати автоматизовані інструменти та метод аудиту вразливостей, що дозволяє виявляти загрози за прийнятний час та з наявними ресурсами. На основі поєднання цих методів розроблено методику, що складається з послідовності блоків, кожен з яких містить етапи збору та обробки інформації. Ефективність методики оцінюється за кількістю виявлених загроз, швидкістю їх виявлення.

Практично використано розроблено методику для експрес-аудиту вразливостей керуючого центру СОД. Отримані результати підтвердили, що методика забезпечує реальні можливості для отримання достовірних оцінок вразливостей систем обробки даних. У статті наведено дані результатів обробки інформації кожним блоком методики під час експрес-аудиту.

Дослідження також показало, що методику можна ефективно використовувати для швидкої оцінки стану безпеки інформаційних систем і постійного моніторингу, що дозволяє оперативно реагувати на нові загрози та забезпечувати високий рівень інформаційної безпеки в реальних ситуаціях сьогодення.

Список літератури

1. Макаренко С. І. Аудит інформаційної безпеки: основні етапи, концептуальні засади, класифікація заходів. *Системи управління, зв'язку та безпеки*. 2018. № 1. С. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf
2. Закон України «Про основні засади забезпечення кібербезпеки України». *Відомості Верховної Ради.* 2017. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Про нейтралізацію загроз інформаційній безпеці держави» № 151/2022. Верховна Рада України: офіційний вебпортал парламенту України. URL: https://zakon.rada.gov. ua/laws/show/151/2022#Text
4. Рішення «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», введено в дію Указом Президента України від 19.03.2022 року № 152/2022. Верховна Рада України: офіційний вебпортал парламенту України. URL: https://zakon.rada.gov. ua/laws/show/n0004525-22#n2
5. Борсуковський Ю. В., Борсуковська В. Ю. Прикладні аспекти захисту інформації в умовах обмеженого фінансування. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2018. №1(1). С.26-34. URL: https://doi.org/10.28925/2663-4023.2018.1
6. Макаренко С.І., Смирнов Г.Є. Модель аудиту захищеності об'єкта критичної інформаційної інфраструктури тестовими інформаційно-технічними впливами. *Труди навчальних закладів зв'язку*. 2021. Т. 7. №1. С. 94–104. DOI:10.31854/1813-324X-2021-7-1-94-104

7. Огірко О.І., Крамар М.О. Аудит інформаційних систем і технологій як інструмент стратегічного управління підприємством. *Law & Sciences = Право та науки.* 2018. № 2. С.26-31.
8. Матюха М. М. Комп'ютерний аудит: опор. курс лекцій для студ. екон. спец. дистанційної форми навчання. К.: ДП «Вид. дім «Персонал», 2018. 228 с.
9. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. Монографія. К: ДУТ, 2015. 124 с.
10. Корченко А. О. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія. Київ: ЦП «Компринт», 2019 . 361 с.

EXPRESS AUDIT AS A TOOL FOR ASSESSING VULNERABILITIES IN INFORMATION SYSTEMS: APPROACHES, METHODOLOGIES, AND RECOMMENDATIONS

O. A. Syropiatov, L. M. Tymoshenko, I. V. Nazarova, N. G. Kozachenko

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

The article is devoted to the research and development of a methodology for express audits of data processing systems for information security. The main attention is paid to the following aspects. Comparative analysis of ISS audit methods. A review and analysis of existing approaches to information security audits is carried out in order to select the most suitable methods for use in a rapid audit. It is concluded that it is best to combine automated tools and vulnerability audits to perform a rapid audit to ensure effective threat detection with minimal time and resources. Development of a rapid audit methodology. An approach to quickly obtain a reliable assessment of the ability of a data processing system to withstand modern threats is presented. The methodology is focused on the rapid identification of vulnerabilities and risk assessment. The methodology consists of a sequential chain of blocks, each of which contains stages of collecting and processing incoming information, after which the data is transferred to the next block for further processing and use. The methodology allows forming a clear structure for assessing the current state of information security, identifying vulnerabilities, and timely adjusting security policies to minimize potential risks. Application of the methodology. An express audit of the control center of the BMS of an enterprise actively involved in logistics operations was practically performed. At the stage of analysis, the system structure, hardware specification, software licensing and updating, etc. are considered. The article provides practical recommendations for improving information security processes based on the results of the express audit. The results of the study show that it is possible to use the rapid audit methodology for a quick assessment of the security status of information systems and for continuous security assessment, which allows one to respond quickly to new threats.

Keywords: rapid audit, information security, data processing systems, audit methodology, vulnerabilities, automated tools, risks